

(19)

Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 0 844 549 A1

(12)

EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
27.05.1998 Patentblatt 1998/22

(51) Int. Cl.⁶: G06F 1/00

(21) Anmeldenummer: 97119971.6

(22) Anmeldetag: 14.11.1997

(84) Benannte Vertragsstaaten:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC
NL PT SE
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(72) Erfinder:
Umkehrer, Alfred, Dipl. Ing. (TU)
87659 Hopferau (DE)

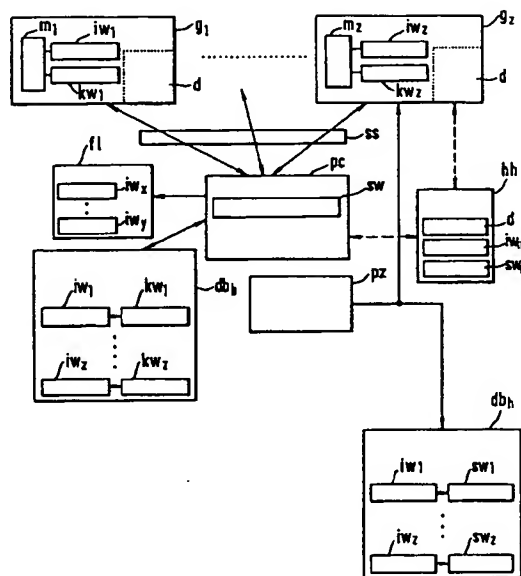
(74) Vertreter:
Morstadt, Volker, Dipl.-Ing.
c/o Endress + Hauser Flowtec AG
Kägenstrasse 7
Postfach 435
4153 Reinach BL 1 (CH)

(30) Priorität: 22.11.1996 EP 96810819

(71) Anmelder:
Endress + Hauser Wetzer GmbH + Co. KG
D-87484 Nesselwang (DE)

(54) Verfahren zum Schutz von Software

(57) Das Verfahren verhindert die unerlaubte Benutzung der von einem Hersteller stammenden Software (sw), die aufgrund einer vom ihm erteilten Einzel-Benutzungserlaubnis für die jeweilige Elektroniksteuerung von gleichen, von ihm stammenden Geräten (g₁; g₂) eines Besitzers verwendbar ist. Die Software ist in einem Computer (pc) des Besitzers installiert und verarbeitet von den Geräten stammende Daten (d), die. Jedem Gerät wird vom Hersteller ein individuelles Identifikationswort (iw₁; iw₂) zugeordnet und in einem nicht-flüchtigen Gerät-Speicher (m₁; m₂) abgelegt. Mittels eines Hersteller-Prozessors (pz) wird aus dem Identifikationswort ein Schlüsselwort (kw₁; kw₂) gebildet, in das ein Benutzungserlaubniswort einbezogen sein kann, und im Gerät-Speicher abgelegt. Beide Wörter werden in einer Datenbank (db_b) des Geräte-Besitzers und in einer Datenbank (db_h) des Software/Geräte-Herstellers aufgelistet. Bei jeder Geräte-Inbetriebnahme überprüft die Software, ob das im Speicher abgelegte Identifikationswort in der Besitzer-Datenbank vorhanden ist. Wenn dies zutrifft wird geprüft, ob darin das zum Identifikationswort gehörende Schlüsselwort vorhanden ist. Wenn dagegen das Identifikationswort darin nicht vorhanden oder wenn das darin vorhandene Schlüsselwort falsch ist, wird geprüft, ob im Gerät-Speicher ein richtiges Schlüsselwort abgelegt ist. Wenn dies zutrifft, legt die Software die beiden Wörter in der Besitzer-Datenbank ab und gibt die Daten-Verarbeitung sowie die Elektroniksteuerung frei, wenn dies dagegen nicht zutrifft, erstellt die Software eine Fehlliste (fl) und gibt die Daten-Verarbeitung und die Elektroniksteuerung nicht frei.



EP 0 844 549 A1

Beschreibung

Die Erfindung betrifft ein Verfahren zum Schutz einer von einem Hersteller stammenden Software gegen unerlaubte Benutzung.

In der US-A 55 02 831 ist ein Verfahren zum Schutz von von einem Hersteller stammenden gleichartigen Empfangsgeräten (dort als communication units bezeichnet) eines Kommunikationssystems gegen unerlaubte Modifizierungen beschrieben, welche Empfangsgeräte mehrere Elektronik-Untereinheiten (dort als operational platforms bezeichnet), z.B. Platten mit gedruckten Schaltungen oder Trägermodule für die Gesamtschaltung (dort als assembly modules supporting the circuitry bezeichnet), umfassen, die ihrerseits für die Funktion der Empfangsgeräte erforderliche Teilssoftware, z.B. für einen digitalen Signalprozessor oder für einen Verschlüsselungs/Entschlüsselungs-Prozessor, enthalten, welches Verfahren folgende Schritte umfaßt:

- jeder Elektronik-Untereinheit und jeder Teilssoftware wird vom Hersteller ein eigenes Untereinheit-Identifikationswort (dort als unit platform identification code bezeichnet) und ein eigenes Teilssoftware-Identifikationswort (dort als serial number of software program bezeichnet) zugeordnet,
- aus den Untereinheit-Identifikationswörtern eines Empfangsgeräts werden ein Elektronik-Identifikationswort (dort als communication unit's hardware identification code bezeichnet), aus den Teilssoftware-Identifikationswörtern desselben Empfangsgeräts ein Software-Identifikationswort (dort als communication unit's software identification code bezeichnet) gebildet und aus dem Elektronik- sowie dem Teilssoftware-Identifikationswort ein Geräte-Identifikationswort (dort als assembly code for the communication unit identification code bezeichnet) gebildet und diese in einem nichtflüchtigen Speicher des Empfangsgeräts gespeichert,
- die Geräte-Identifikationswörter werden laufend zu einer Datenbank des Herstellers der Empfangsgeräte übertragen und dort aufgelistet, und
- bei jeder Modifikation eines Empfangsgeräts wird diese aufgrund des durch die Modifikation veränderten Geräte-Identifikationsworts erkannt.

Bei diesem Verfahren geht es im Gegensatz zum Verfahren der Erfindung also lediglich um das Erkennen und Melden von nicht erlaubten Manipulationen an Empfangsgeräten des Kommunikationssystems, wobei der Verschlüsselungs/Entschlüsselungs-Prozessor offensichtlich nicht in den Schutz gegen unerlaubte Modifizierungen einbezogen ist.

Demgegenüber ist es ein Ziel der Erfindung, daß eine von einem Hersteller geschaffene Software, also ein sogenanntes Software-Paket, von einem Erwerber nur zusammen mit demjenigen Gerät desselben Her-

stellers benutzbar sein soll, mit dem zusammen und für das sie/es erworben worden ist. Es soll also dem Besitzer von Gerät und Software-Paket nicht möglich sein, weitere gleichartige Geräte ohne die Verpflichtung zu erwerben, auch das für jedes weitere Gerät erforderliche Software-Paket erwerben zu müssen.

Die Erfindung geht von dem Grundgedanken aus, daß sich diese Verpflichtung nur durchsetzen läßt, wenn das System sie von selbst erzwingt, und erreicht dies dadurch, daß ein zu einem erworbenen Gerät passendes Software-Paket zusammen mit einem anderen Gerät nicht funktionsfähig ist, sondern es erst wird, wenn eine weitere Benutzungserlaubnis erworben worden ist.

Somit besteht die Erfindung in einem Verfahren zum Schutz einer von einem Hersteller stammenden Software gegen unerlaubte Benutzung, welche Software

- aufgrund einer vom Hersteller erteilten Einzel-Benutzungserlaubnis für eine Elektroniksteuerung eines einzelnen von gleichartigen, vom Hersteller stammenden Geräten eines Besitzers verwendbar ist,
- in einem Computer des Besitzers installiert ist und einer Verarbeitung von Daten dient, die von den Geräten stammen, welches Verfahren folgende Schritte umfaßt:
- jedem Gerät wird vom Hersteller ein individuelles Identifikationswort zugeordnet, das sich von den jeweiligen Identifikationswörtern aller anderen Geräte unterscheidet;
- das jeweilige Identifikationswort wird in einem nichtflüchtigen Speicher des jeweiligen Geräts gespeichert;
- vom Hersteller wird mittels eines Prozessors aus dem jeweiligen Identifikationswort anhand eines nur ihm bekannten Verschlüsselungs-Algorithmus ein Schlüsselwort gebildet und im Speicher des jeweiligen Gerätes gespeichert;
- die Identifikationswörter werden zusammen mit dem zugehörigen jeweiligen Schlüsselwort in einer Datenbank des Besitzers der Geräte und in einer Datenbank des Herstellers der Software und der Geräte aufgelistet;
- bei jeder Inbetriebnahme eines der Geräte überprüft die Software,

-- ob das im Speicher dieses Geräts abgelegte Identifikationswort in der Datenbank des Besitzers vorhanden ist,

-- wenn dies zutrifft, ob in der Datenbank des Besitzers das zu diesem Identifikationswort gehörende Schlüsselwort vorhanden ist,

-- wenn dagegen das Identifikationswort in der Datenbank des Besitzers nicht vorhanden oder wenn das in der Datenbank des Besitzers vorhandene Schlüsselwort falsch ist, ob im Spei-

cher des Geräts ein richtiges Schlüsselwort abgelegt ist;

- trifft dies zu, legt die Software das Schlüsselwort zusammen mit seinem zugehörigen Identifikationswort in der Datenbank des Besitzers ab und gibt die Elektroniksteuerung des Gerätes und die Verarbeitung der Daten frei;
- trifft dies dagegen nicht zu, erstellt die Software eine Fehlliste derjenigen Identifikationswörter, zu denen jeweils ein falsches Schlüsselwort gehört, und gibt die Elektroniksteuerung des Gerätes und die Verarbeitung der Daten nicht frei.

Nach einer Weiterbildung der Erfindung wird in das Schlüsselwort ein Benutzungserlaubniswort aufgenommen.

Nach einer Ausgestaltung der Erfindung wird zwischen den Geräten und dem Computer eine serielle und/oder parallele Schnittstelle vorgesehen.

Nach einer anderen Ausgestaltung der Erfindung wird zwischen den Geräten und dem Computer eine manuell gesteuerte Datenübernahme aus den Geräten in ein Hilfsgerät vorgesehen.

Die Erfindung wird nun anhand der Figur der Zeichnung näher erläutert, die nach Art eines Blockschaltbilds das Zusammenwirken einzelner Komponenten beim Ablauf des Verfahrens der Erfindung veranschaulicht.

In der Figur sind von einer beliebigen Anzahl von untereinander gleichartigen, insb. gleichen, Geräten, z.B. Meßgeräten oder Registriergeräten, ein erstes Gerät g_1 und ein letztes Gerät g_z dargestellt. Die Geräte stammen von ein und demselben Hersteller und befinden sich zur Nutzung und Verwendung bei ein und demselben Besitzer.

Zum Lieferumfang der Geräte gehört auch eine Software sw, die der Hersteller der Geräte vollständig selbst geschaffen oder durch Bearbeitung von Standard-Software auf die Anwendung zusammen mit den Geräten zugeschnitten hat. Die Software sw läuft auf einem Computer pc des Besitzers der Geräte und dient u.a. deren Elektroniksteuerung.

Im Rahmen dieser Steuerung erlaubt die Software z.B. einen Austausch von Daten d zwischen den Geräten und dem Computer. Die Daten d werden von jedem Gerät aufgrund von irgendwelchen Messungen, z.B. einer Messung von Druck, pH-Wert, Temperatur, Durchfluß oder Gasen etc., erzeugt.

Das Zusammenwirken des Computers pc mit den Geräten kann z.B. über eine serielle und/oder eine parallele Schnittstelle ss, also eine dauernde Leitungsverbindung, erfolgen, die in der Figur durch ausgezogene Zwei-Richtungspfeile veranschaulicht ist.

Eine andere Möglichkeit der Datenverbindung zwischen den Geräten und dem Computer pc ist in der Figur ebenfalls, jedoch mittels gestrichelt gezeichneter Zwei-Richtungspfeile dargestellt: In ein Hilfsgerät hh mit

einem schreib- und lesbaren Datenträger, wie z.B. ein Cassettenrecorder, werden die Daten d aus den Geräten vor Ort durch manuelle Betätigung eingelesen. Danach wird das Hilfsgerät hh an den Ort des Computers pc gebracht, und dort werden die Daten d in ihn über eine geeignete Verbindung eingelesen.

Die Daten d können durch den Computer pc mittels der Software sw zu einer Anzeige der Meßwerte verarbeitet werden..

Der Hersteller der Geräte und der eigengeschaften Software hat ein Interesse daran, daß "seine" Software nur gegen Bezahlung benutzt wird, daß sie also nur mit demjenigen Gerät benutzt werden kann, mit dem zusammen und für das sie vom Besitzer des Geräts erworben worden ist.

Eine unerwünschte und somit aus der Sicht des Herstellers unerlaubte Benutzung der Software sw liegt somit schon dann vor, wenn der Besitzer eines oder mehrerer schon erworbener Geräte z.B. ein zu einem späteren Zeitpunkt erworbenes Gerät durch Kopieren der Software eines schon erworbenen Geräts benutzen könnte.

Der Hersteller der Geräte und der zugehörigen Software sw ist daher gezwungen, jedes einzelne zu einem Gerät gehörende Software-Paket mit einer Art von Einzel-Benutzungserlaubnis zu versehen. Es ist also erforderlich, das einzelne Gerät und die zu ihm "gehörende" Software so miteinander zu verknüpfen, daß ausschließlich diese beiden zusammenarbeiten können.

Entsprechend dem Verfahren der Erfindung wird dies wie folgt erreicht: Der Hersteller ordnet jedem Gerät g_1 , g_z ein individuelles und somit geräte-spezifisches Identifikationswort iw_1 , iw_z derart zu, daß sich alle Identifikationswörter voneinander unterscheiden. Jedes geräte-spezifische Identifikationswort iw_1 , iw_z wird in einem nichtflüchtigen Speicher m_1 , m_z des jeweiligen Geräts g_1 , g_z gespeichert.

Vom Hersteller wird ferner aus dem jeweiligen Identifikationswort iw_1 , iw_z mittels eines Prozessors pz anhand eines nur ihm bekannten, geheimzuhaltenden und somit hier nicht offenzulegenden Verschlüsselungs-Algorithmus ein Schlüsselwort kw_1 , kw_z gebildet und im zugehörigen Speicher m_1 , m_z des jeweiligen Gerätes g_1 , g_z ebenfalls gespeichert.

Zur Veranschaulichung möge ein Identifikationswort iw_1 und ein Identifikationswort iw_z in Dezimaldarstellung lauten: $iw_1 = 123456$; $iw_z = 234561$. Die Schlüsselwörter kw_1 , kw_z könnten dann lauten: $kw_1 = 132537495116$, $kw_z = 253749511671$; diese sind dadurch gebildet worden, daß zwischen zwei benachbarten Ziffern deren Summe eingefügt worden ist.

Nach einer Weiterbildung der Erfindung ist es auch möglich, in das Schlüsselwort kw_1 , kw_z ein Benutzungserlaubniswort mit einzubeziehen. Durch diesen "Einbau" können verschiedene Arten oder Grade von Benutzungserlaubnissen erteilt werden, die z.B. an der Komplexität der Datenverarbeitung der Software sw ori-

entiert sind. Ist eine solche Staffelung nicht erforderlich, so stellt das mittels des Verschlüsselungs-Algorithmus gebildete Schlüsselwort selbst die Benutzungserlaubnis dar.

Als Verschlüsselungs-Algorithmus kann irgendein in der digitalen Verschlüsselungstechnik üblicher Algorithmus verwendet werden.

Die Identifikationswörter werden ferner zusammen mit dem zugehörigen jeweiligen Benutzungserlaubniswort in einer Datenbank db_b des Besitzers der Geräte und in einer Datenbank db_h des Herstellers der Software und der Geräte aufgelistet. Die Datenbank db_b des Besitzers der Geräte ist in der Figur separat dargestellt, jedoch selbstverständlich Bestandteil des Computers pc.

Da es sich bei der Datenbank db_b des Besitzers der Geräte und der Datenbank db_h des Herstellers der Software und der Geräte um zwei von einander unabhängige Datenbanken handelt, ist zwischen ihnen in der Figur keine Datenverbindung gezeichnet.

Bei jeder Inbetriebnahme eines der Geräte überprüft nun die Software sw, ob das im Speicher m_1 , m_2 dieses Geräts g_1 , g_2 abgelegte Identifikationswort iw_1 , iw_2 in der Datenbank db_b des Besitzers vorhanden ist. Wenn dies zutrifft, überprüft die Software sw anschließend, ob in der Datenbank db_b das zu diesem Identifikationswort gehörende Schlüsselwort kw_1 , kw_2 vorhanden ist.

Wenn dagegen das Identifikationswort iw_1 , iw_2 in der Datenbank db_b nicht vorhanden oder wenn das darin vorhandene Schlüsselwort falsch ist, überprüft die Software sw anschließend, ob im Speicher m_1 , m_2 des Geräts ein Schlüsselwort kw_1 , kw_2 abgelegt ist. Trifft dies zu, legt die Software sw das Schlüsselwort kw_1 , kw_2 zusammen mit seinem zugehörigen Identifikationswort iw_1 , iw_2 in der Datenbank db_b des Besitzers ab und gibt erst jetzt die Elektroniksteuerung des Gerätes und die Verarbeitung der Daten frei.

Trifft es dagegen nicht zu, daß im Speicher m_1 , m_2 des Geräts ein Schlüsselwort kw_1 , kw_2 abgelegt ist, erstellt die Software sw eine Fehlliste fl derjenigen Identifikationswörter iw_x , iw_y , zu denen jeweils ein falsches Schlüsselwort gehört, und gibt die Elektroniksteuerung des Gerätes und die Verarbeitung der Daten nicht frei.

Die Fehlliste fl informiert den Besitzer der Geräte somit darüber, für welche Geräte er eine Benutzungserlaubnis noch erwerben muß. Die Fehlliste fl ist wieder Bestandteil des Computers pc. Sie kann in geeigneter Form an den Hersteller der Geräte übermittelt werden, um die fehlenden Benutzungserlaubnisse zu ordern.

Auch bei teilweisem oder vollständigem Datenverlust der Identifikations- und der Schlüsselwörter beim Besitzer ist die Fehlliste fl von Nutzen. In diesem Fall ermittelt der Hersteller der Software sw durch Vergleich der Fehlliste fl mit dem Inhalt seiner Datenbank db_h , für welche Geräte schon Benutzungserlaubnisse erworben worden waren, und erteilt diese dem Besitzer der Geräte erneut, jedoch z.B. kostenlos.

Patentansprüche

1. Verfahren zum Schutz einer von einem Hersteller stammenden Software (sw) gegen unerlaubte Benutzung, welche Software

- aufgrund einer vom Hersteller erteilten Einzel-Benutzungserlaubnis für eine Elektroniksteuerung eines einzelnen von gleichartigen, vom Hersteller stammenden Geräten (g_1 ; g_2) eines Besitzers verwendbar ist,
- in einem Computer (pc) des Besitzers installiert ist und
- einer Verarbeitung von Daten (d) dient, die von den Geräten stammen, welches Verfahren folgende Schritte umfaßt:
- jedem Gerät (g_1 ; g_2) wird vom Hersteller ein individuelles Identifikationswort (iw_1 ; iw_2) zugeordnet, das sich von den jeweiligen Identifikationswörtern aller anderen Geräte unterscheidet;
- das jeweilige Identifikationswort wird in einem nichtflüchtigen Speicher (m_1 ; m_2) des jeweiligen Geräts (g_1 ; g_2) gespeichert;
- vom Hersteller wird mittels eines Prozessors (pz) aus dem jeweiligen Identifikationswort anhand eines nur ihm bekannten Verschlüsselungs-Algorithmus ein Schlüsselwort (kw_1 ; kw_2) gebildet und im Speicher des jeweiligen Gerätes gespeichert;
- die Identifikationswörter werden zusammen mit dem zugehörigen jeweiligen Schlüsselwort in einer Datenbank (db_b) des Besitzers der Geräte und in einer Datenbank (db_h) des Herstellers der Software und der Geräte aufgelistet;
- bei jeder Inbetriebnahme eines der Geräte überprüft die Software,
 - ob das im Speicher dieses Geräts abgelegte Identifikationswort in der Datenbank des Besitzers vorhanden ist,
 - wenn dies zutrifft, ob in der Datenbank des Besitzers das zu diesem Identifikationswort gehörende Schlüsselwort vorhanden ist,
 - wenn dagegen das Identifikationswort in der Datenbank des Besitzers nicht vorhanden oder wenn das in der Datenbank des Besitzers vorhandene Schlüsselwort falsch ist, ob im Speicher des Geräts ein richtiges Schlüsselwort abgelegt ist;
- trifft dies zu, legt die Software das Schlüsselwort zusammen mit seinem zugehörigen Identifikationswort in der Datenbank des Besitzers ab und gibt die Elektroniksteuerung des Gerätes und die Verarbeitung der Daten frei;

- trifft dies dagegen nicht zu, erstellt die Software eine Fehlliste (fl) derjenigen Identifikationswörter (iw_x ; iw_y), zu denen jeweils ein falsches Schlüsselwort gehört, und gibt die Elektroniksteuerung des Gerätes und die Verarbeitung der Daten nicht frei. 5
- 2. Verfahren nach Anspruch 1, bei dem in das Schlüsselwort (kw_1 ; kw_2) ein Benutzungserlaubniswort aufgenommen wird. 10
- 3. Verfahren nach Anspruch 1 mit einer seriellen und/oder parallelen Schnittstelle zwischen den Geräten (g_1 ; g_2) und dem Computer (pc). 15
- 4. Verfahren nach Anspruch 1 mit einer manuell gesteuerten Datenübernahme aus den Geräten (g_1 ; g_2) in ein Hilfsgerät (hh). 20

20

25

30

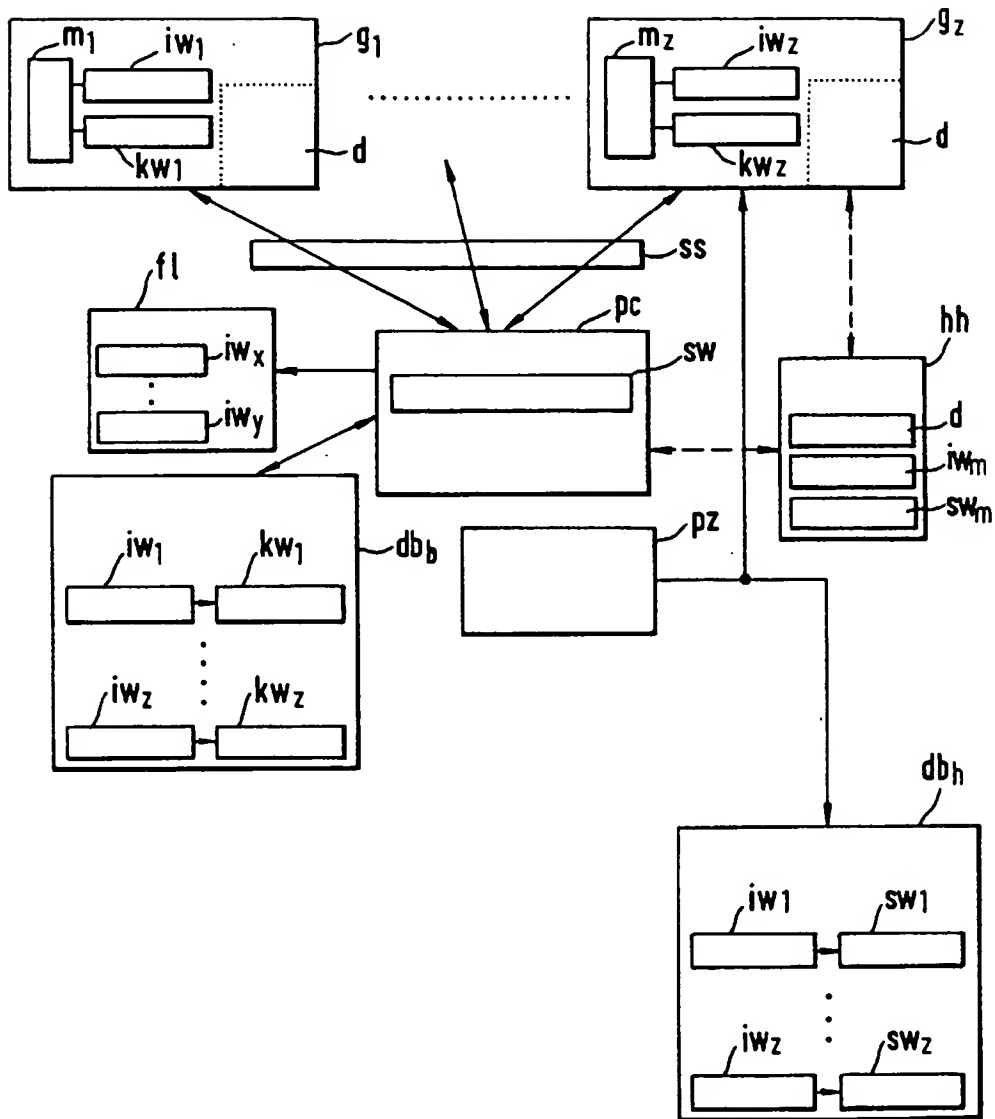
35

40

45

50

55





Europäisches
Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 97 11 9971

EINSCHLÄGIGE DOKUMENTE			
Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.Cl.6)
A	US 5 379 343 A (GRUBE GARY W ET AL) 3. Januar 1995 * Spalte 2, Zeile 61 - Spalte 4, Zeile 35 * * Spalte 5, Zeile 11 - Zeile 60; Abbildungen 1,2,4 *	1	G06F1/00
D,A	US 5 502 831 A (GRUBE GARY W ET AL) 26. März 1996 * Spalte 2, Zeile 37 - Spalte 5, Zeile 9; Abbildungen *	1	
			RECHERCHIERTE SACHGEBIETE (Int.Cl.6)
			G06F
Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt			
Recherchenort DEN HAAG		Abschlußdatum der Recherche 26. Februar 1998	Prüfer Moens, R
<p>KATEGORIE DER GENANNTEN DOKUMENTE</p> <p>X : von besonderer Bedeutung allein betrachtet Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie A : technologischer Hintergrund O : nichtschriftliche Offenbarung P : Zwischenliteratur</p> <p>T : der Erfindung zugrunde liegende Theorien oder Grundsätze E : älteres Patentedokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist D : in der Anmeldung angeführtes Dokument L : aus anderen Gründen angeführtes Dokument & : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument</p>			

EPO FORM 1503 03.82 (Pd/C03)